Remarks

As previously stated in this amendment, amendments to the drawings have been made prior to the formal set of drawings being filed with the Patent and Trademark Office. The set of formal drawings that was submitted with the Notice to File Corrected Application Papers on June 26, 2001, (and received by the PTO on June 28, 2001) are correct and contain all of the drawing changes made to the informal set of drawings (which were filed with the application on December 19, 2000). The updates included in the formal set of drawings filed are listed below :

In Figure 8, second row, PE_3 (X-Phase), reference numeral 20 was incorrect and has been updated to 200; in Figure 14, Register BN reference numeral 272 has been updated to 298 in two occurrences; and in Figure 16, the last number in the column on the right-hand bottom side has been updated to 24, not 34, as originally depicted in the informal set of drawings filed with the patent application. Please note that Figure 13 has been split by the draftsperson into Figures 13A and 13B, respectively. In the specification, where Figure 13 is mentioned, it is to be considered as encompassing both Figures 13A and 13B inclusively.

At present claims 1-10 stand rejected under 35 U.S.C. § 101. Additionally, claim 1 is objected to as are also claims 6 and 7. Claims 6-10 are rejected under 35 U.S.C. § 102 based upon the patent to Monier (US Patent Number 5,764,554 issued June 9, 1998, and having a foreign application priority date of November 8, 1994). Lastly, claims 1-5 also stand rejected under 35 U.S.C. § 103(a) based upon the same patent to Monier. In light of the comments presented below and the amendments made to applicants' claims herein, all of these objections and rejections are respectfully traversed. Accordingly, claims 1-10 remain present in the current application.

For ease in understanding, it is noted that the objections and rejections set forth by the Examiner are considered herein in the same order as presented in the above-mentioned Office Action. Furthermore, as a matter of formality, it is noted that the form PTOL-326 (Office Action Summary) provided by the Examiner appears to have left box 6 unchecked. Nonetheless, this line in the form does indicate that claims 1-10 is/are rejected. It is assumed that the Examiner intended to put a check mark in box 6.

Attention is first directed to the rejection of applicants' claims 1-10 under 35 U.S.C. § 101. In this regard, the Examiner has indicated that "the language of the claims 1, 3, 5, 6 and 7 raises a question as to whether the claim is directed merely to an abstract idea that is not tied to a technological art, environment, or machine which would result in a practical application producing a concrete, useful, and tangible result to form the basis of statutory subject matter under 35 USC § 101." This rejection is respectfully but strenuously traversed.

With respect to the rejection under 35 U.S.C. § 101, it is noted that claim 1 refers to a number of non-abstract components and elements. For example, claim 1 refers to "storing said value Z_0 in a first register and in a second register." Claim 1 also talks about providing a signal representing a particular constant. Signals are physical things, not abstract entities. If signals were abstract entities, human beings could safely stand in front of military radar dish transmitters. Claim 3 likewise has similar recitations. Claim 5 recites the operation of repeatedly operating a circuit which performs a certain modulo N operation. Clearly and unequivocally, circuits are not abstract entities nor pure mathematical algorithms. Likewise, applicants' claim 7 refers to modular multiplication circuits and multiplexor circuits. Accordingly, it is seen that all of applicants' claims, and particularly the ones recited by the Examiner, refer to actual physical entities and processes.

Carried to its logical conclusion, the Examiner's characterization of applicants' claims would lead one to believe that merely because a digital circuit carries out the operation of adding two integers, such circuits are not worthy of patentable protection. Clearly, the history of our patent system flies in the face of this result. Merely because a circuit carries out an operation which is arithmetic in nature does not make that circuit unpatentable. To deny that applicants' claimed apparatus and methods are related to mathematical operations would be pointless, fruitless and inaccurate. Nonetheless, it is clearly seen that applicants' claims are stated and framed in terms of physical quantities and entities. It is furthermore seen that circuits for carrying out modulo N exponentiation operations have proven themselves to be extremely desirable and valuable in the transmission of digital signals which must be encrypted and decrypted. The fact that such specific methods and devices have a foundation in an underlying mathematical theory provides absolutely no foundation whatsoever for denying patentability to circuits and methods for carrying out these operations. Accordingly, it is seen that the Examiner's rejection of applicants' claims under 35 U.S.C. § 101 is not in any way well founded. It is therefore respectfully requested that this rejection be withdrawn.

Claim 1 is objected to because applicants refer to "the constant, *C*" rather than to "a constant, *C*." In this regard, it is noted that applicants have acquiesced in the objection. However, it is applicants' position that this change is both unnecessary and undesirable and does not in any way change, affect or vary the scope of applicants' claims. In this regard, the Examiner's attention is directed to the following example. Suppose that one had a claim which read in part as follows:

> generating a first binary signal A;
> generating a second binary signal B; and
> generating a binary signal representing the sum of signal A and signal B.

Those of ordinary skill in the art would fully and completely understand the structure and nature of this claim even though there was a recitation to "the sum." In this particular case, the addition operation produces an inherent result. There is no "a sum" to be selected from a whole bunch of possibly different sums. In his rejection of applicants' claims under 35 U.S.C. § 101, the Examiner has impliedly asserted that the inventions to which claims are directed must be tied to the technological arts. The technological arts are necessarily, essentially and fundamentally connected to the science of physics. Furthermore, the language of the science of physics is mathematics. Those of ordinary skill in the art necessarily having a bent towards the technological arts would in fact be confused by a recitation of "a sum." They would ask "What other sums are possible?" Accordingly, it is applicants' attorney's position that the Patent and Trademark Office should cease and desist from the strict adherence to antecedent basis rules when it comes to certain mathematical expressions such as "the sum of," "the product of," "the integral of," etc.

In sum then, while applicants have acceded to the Examiner's objection for reasons of expediency, it is nonetheless argued and asserted that this change is not only unnecessary and confusing but is not intended in any way whatsoever to modify, adjust, vary or change the scope of applicants' claims.

Attention is next directed to the Examiner's objections to the applicants' spelling of the word multiplexor. In this regard, it is noted that multiplexor is an acceptable spelling variant of the word multiplexer. In support of this position, applicants are enclosing photocopies of the pages of two dictionaries both of which support the position that the word multiplexor is an acceptable variant of the spelling for multiplexer. Accordingly, in this regard, no amendment to applicants' claims is necessary.

Attention is next direct to the rejection of applicants' claims 6-10 under 35 U.S.C. § 102(b) based upon the aforementioned patent to Monier. In this regard, it is noted

that applicants' claims 6-10 are directed to an apparatus for computing A^E modulo N. In short, applicants' claims 6-10 are directed to exponentiation operations modulo N. In contrast, even though based upon some of the same Montgomery algorithm principles for modular arithmetic without the division, the cited patent is not directed to circuits for performing modular exponentiation operations. Rather, as stated in the abstract, the patent is directed to a method for implementing modulo N reduction. This is a much simpler process than modulo N multiplication and, accordingly, a priori, even a more simple process than exponentiation modulo N. Accordingly, since the circuits for performing these operations are not taught, disclosed or suggested in the patent to Monier, the rejection of applicants' claims 6-10 under 35 U.S.C. § 102 is not well founded. More particularly, it is pointed out that applicants' claim 6 for example includes a means for controlling input operand selection to a circuit so that after at most t iterations, the output result of the circuit is A^E modulo N. In this case, t represents the size in bits of the integer N. No such control means are provided in the patent to Monier. For these reasons, it is seen that the rejection of applicants' claims 6-10 under 35 U.S.C. § 102 should be withdrawn.

Additionally, in amplification of the above comments, the Examiner's attention is directed to column 5, lines 63-64, of the cited patent wherein it is stated that the circuit shown in Monier's Figure 2 is used to produce an error correction parameter H which is a binary data element. In column 1, lines 50-55 clearly teach that $H = 2^{mk} \bmod N$. This is not the output of applicants' claimed apparatus or process. Additionally, it is noted that in column 5, lines 24-25, of the cited patent, Monier specifically indicates that the circuit of his Figure 1 enables the invention to be implemented. In this regard, attention is again drawn to the abstract and to column 1, lines 7-11, where it is again clearly stated that the invention is directed to a method for implementing modulo N reduction operations according to the Montgomery algorithm. Similarly, in support of the above positions, the Examiner's attention is also directed to Figure 3, Figure 4, Figure 5 and Figure 6 in the subject patent, all of which clearly show as their last step the production

of the value *C* mod *N*. Again it is clearly, unequivocally stated that the essential and sole purpose of the subject patent is the performance of modulo *N* reduction operations. It does not even appear to teach modulo *N* multiplication, and it certainly does not teach structures, devices or methods for performing modulo *N* exponentiation operations. For these reasons also, it is seen that the rejection of applicants' claims 6-10 under 35 U.S.C. § 102 cannot be sustained. It is therefore respectfully requested that this rejection be withdrawn.

With respect to the Examiner's comments concerning applicants' claim 8 and the reference to column 5, lines 47-55, of the patent to Monier, it is first of all noted that this particular section of the cited patent, while it may describe a circuit that is capable of exhibiting more than one state, this is the entire extent of the teachings. The teaching of such a circuit having a state which can be used as an output is not the same as teaching that there is provided a finite state machine as a control element. A flip-flop does not a finite state machine make. Furthermore, even if the cited portion of the patent to Monier were to refer to a finite state machine, it certainly is not anything that is connected or utilized in the fashion as in applicants' claimed invention to produce modulo *N* exponentiation as an output result.

With respect to Examiner's reference to claim 9, the inclusion of a counter which counts from 0 to some finite value, even if present and counting to the same number, does not disclose a counter which is part of a finite state machine which is part of a control unit which is used in conjunction with a modulo *N* multiplication engine which is used to perform modulo *N* exponentiation operations.

With respect to Examiner's reference to claim 10, it is noted that the same comments apply here as apply with respect to the Examiner's comments concerning claim 8 which have been addressed above.

Attention is next directed to the rejection of applicants' claims 1-5 under 35 U.S.C. § 103(a) based upon the patent to Monier. In this regard, it is noted that applicants' claims 1-5, as with applicants' claims 6-10, are directed to methods and systems for performing exponentiation operations modulo an integer *N*. With respect to the art cited by the Examiner, the art is seen to teach merely modulo *N* reduction operations. There is no circuit nor method described in the subject patent for producing exponentiation modulo *N* results. In contrast, it is clearly seen that the thrust of the patent to Monier is clearly directed and limited to the simple modulo *N* reduction operation and not to the more complex operations of modulo *N* exponentiation which are at least two levels removed from reduction with respect to the degree of complexity found in Monier. Furthermore, even if the patent to Monier were to teach modulo *N* exponentiation, no where is it taught, disclosed or suggested that the exponent *E* is employed as an input to a device such as a finite state machine for controlling the operation of a specific circuit. In particular, applicants' claims include a recitation to a circuit which accepts two input operands, *A* and *C*, and which produces an output result given by $A\ C\ 2^{-mk}$ modulo *N*. In contrast, the output produced by the circuits and methods shown in Monier produce only *C* modulo *N*. There is no teaching, disclosure or suggestion of how to use their circuits and methods to produce the multiplication product $A\ C\ 2^{-mk}$ modulo *N*. Even if there were such a circuit, and there is not, there is no teaching, disclosure or suggestion of how to use that circuit in conjunction with the values of *A* and *C* and certain constants in a sequential manner to produce the exponential results A^E modulo *N*. Accordingly, it is seen that there is nothing disclosed, suggested or taught by Monier that would lead one of ordinary skill in the art to devise methods or devices for producing modulo exponentiation results. Likewise, it is thus seen that the rejection of applicants' claims 1-5 under 35 U.S.C. § 103 is not well founded. Accordingly, it is therefore respectfully requested that this rejection also be withdrawn.

It is noted that the amendments being made herein are being submitted as of right. It is also noted that the present response does not require the payment of any additional fees except for the payment of a one-month extension of time fee which was necessitated by applicants' representative being engaged in other pressing matters.

No amendment made was related to the statutory requirements of patentability unless expressly stated herein. No amendment made was for the purpose of narrowing the scope of any claim, unless applicant(s) have argued herein that such amendment was made to distinguish over a particular cited document or combination of documents.

Accordingly, it is now seen that all of the applicants' claims are in condition for allowance. Therefore, early notification of the allowability of applicants' claims is earnestly solicited. Furthermore, if there are any other matters which the Examiner feels could be expeditiously considered and which would forward the prosecution of the instant application, applicants' attorney wishes to indicate his willingness to engage in any telephonic communication in furtherance of this objective. Accordingly, applicants' attorney may be reached for this purpose at the numbers provided below.

Respectfully Submitted,

LAWRENCE D. CUTTER, Sr. Attorney
Reg. No. 28,501

IBM Corporation, IP Law Dept.
2455 South Rd., M/S P386
Poughkeepsie, NY 12601

Phone: (845) 433-1172
FAX: (845) 432-9786
EMAIL: cutter@us.ibm.com